IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 9, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.122

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 11, November 2020 ||

A Study on Encryption and Confidentiality in WLAN

Anitha Eemani[1]

Sr. Java Full Stack Developer, National Association of Insurance Commissioners (NAIC), USA[1]

ABSTRACT: The condition wireless social network refers to technology that makes it possible for two or even additional pcs to interact utilizing standard network process, yet without network cabling. Stringently speaking, any technology that does this may be called wireless networking. The notion of modern wireless technology has been around for an extended period, beginning with the first analogue cellular telephones. Technologies existing today are even most ideal identified in the complying with the layout. Devices commonly used for wireless media include mobile computers, desktop, handheld computer systems, personal digital assistants (Personal organizers), cellular phones, pen-based personal computers, as well as pagers.

KEYWORDS: wlan, wireless technologies, encryption

I. WIRELESS TECHNOLOGIES

Wireless networks operate identical to wired networks, having said that, wireless networks have to turn information signals right into a form suited for transmission using the air tool.Ultimately the above technologies, omitting cognate, are pertained to as 11.5 G and also are looked at contending as field professionals assume each modern technology will undoubtedly present highly competitive items. The present fuzzword nevertheless commonly describes a wireless computer network (LANs). This technology, sustained by the development of cross-vendor market criteria such as IEEE 802.11, has made a lot of cost-effective wireless options that are expanding in level of popularity with the company and also schools in addition to advanced applications where network electrical wiring is complicated, including in warehousing or point-of-sale handheld devices.

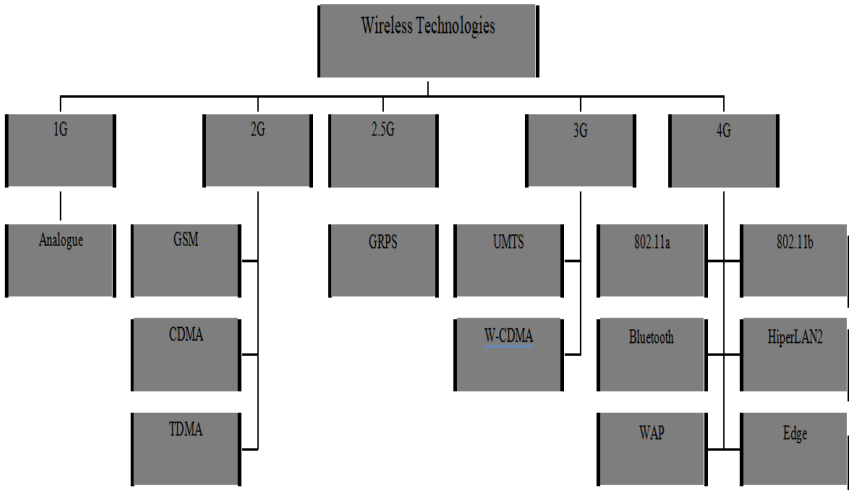


Figure 1

Types of wireless network

An ad-hoc, or peer-to-peer wireless network, features some computer systems each geared up along with a wireless social network user interface card. Each pc can easily connect straight with every one of the other wireless made it possible for personal computers. They can easily discuss documents and also ink-jet printers through this, however, might certainly not have the ability to accessibility wired LAN resources, unless some of the computers function as a link to the wired LAN using a unique software application. (This is named "linking").

A wireless network can additionally make use of an access factor or even a base station. In this sort of system the get access to aspect acts like a hub, supplying connectivity for the wireless computers. It can quickly hook up (or "bridge") the wireless LAN to a wired LAN, permitting wireless computer access to LAN sources, including data web servers or

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 11, November 2020 ||

existing World complete web Connectivity.
Each gets access to factor has a limited assortment within which a wireless link may be maintained between the client pc as well as they get access to point. The actual distance varies hing on the setting; suppliers typically explain both interiors as well as exterior selections to provide a realistic sign of reliable efficiency. Likewise, it needs to be noted that when functioning at the limits of variation, the performance may fall, as the top quality of hookup degrades and also the system recompenses.
Regular interior variations are 150-300 feet but can be shorter if the structure development interferes with radio transmissions. Longer varieties are possible, yet efficiency will diminish along with range.
Outdoor selections are priced estimate up to thousand feet, however again this hinges on the setting.
There are methods to stretch the available operating variety of Wireless interactions, by using more than a single access point or even making use of a wireless relay/ extension factor.
The special gain access to factor capacity depends upon the supplier. Some hardware access factors have a recommended limit of 10 actually, along with various other extra expensive access points supporting approximately one hundred wireless relationships. Utilizing additional computers than suggested are going to create a performance as well as dependability to endure.
Program gain access to aspects may likewise impose customer limitations. However, this relies on the details software application, as well as the range computer's ability to process the needed details.

II. APPLICATIONS

The reach of wireless communication in embedded devices remains to develop. Forrester Study, a provider that focuses on business effects of technology improvement, has reported that in a couple of short years, around 95% of devices used to access the Net will be non-PC devices that use an embedded body.
There are many applications for inserted units along with a Wi-Fi user interface:
Industrial method and also management uses where wired hookups are too costly or even undesirable, e.g., consistently relocating machinery.
Emergency functions that demand instant and transitory create, such as a battlefield or even disaster scenarios.
Mobile applications, like property tracking.
Monitoring video cameras (maybe you perform certainly not desire them conveniently observed, wires are challenging to conceal).
Vertical markets like health care, learning, as well as production.
Communication with various other Wi-Fi units, like a laptop pc or even a PERSONAL ORGANIZER.
Device to Maker (M2M) apps
Concerning the last one, the phrase Machine to Machine (M2M) pertains to technologies that allow each wireless as well as wired bodies to connect with various other gadgets of the very same type. Yet another feature of M2M communication is actually that this affiliation allows mainly automated communication between far-off, distant equipment and one or more coatings of core management apps. It attends to real-time tracking and command without the demand for individual interference.
Depending On to ABI Research study, a modern technology investigation and consultatory organization, much more than 30 billion units are going to be wirelessly connected to the Web of Traits (Web of Every Thing) by 2020.
In the wireless M2M area, there are two primary lessons of interconnections: brief variety and also vast area. The vast principal place modern technology administers embedded cell modules to hook up distant tools to the world wide web or even application web servers. A cell component consists of much of the very same elements that you will find in a mobile, featuring vocal and also records communication, and also is suitable for ingrained applications.
M2M uses discovered within a broad range of markets; these consist of automated meter analysis (AMR), vending makers, factor of sales (POS) terminals, transport as well as strategies (fleet control), medical care, security innovation and numerous various other requests.

III. CONFIDENTIALITY ANDENCRYPTION

WEP was ratified like a Wi-Fi security criterion in September of 1999. The 1st variations of WEP weren't specifically substantial, also for the time they were launched, because UNITED STATE limitations on the export of several cryptographic technologies led to makers restraining their tools to merely 64-bit shield of encryption. When the constraints were elevated, it was enhanced to 128-bit. Despite the overview of 256- bit WEP encryption, 128-bit stays some of the most typical executions.
Regardless of modifications to the protocol as well as an improved secret measurement, in time numerous security flaws were found in the WEP standard and, as computing electrical power improved, it came to be less complicated and

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 11, November 2020 ||

more comfortable to manipulate all of them. As early as 2001 proof-of-principle deeds were floating around and also by 2005, the FBI provided a public presentation (in an attempt to boost understanding of WEP's weak spots) where they cracked WEP codes in mins making use of openly on-call software.
Even with several remodellings, workarounds, as well as other attempts to support the WEP device, it continues to be very vulnerable, and also bodies that rely upon WEP must be improved or even if security upgrades are certainly not a choice, replaced. The Wi-Fi Alliance officially resigned WEP in 2004.

WPA

To take care of vulnerabilities in WEP, the Wi-Fi Collaboration trade group established WPA at the starting point of 2003. One of the most common WPA setups is WPA-PSK (Pre- Shared Trick). The secrets made use of by WPA are 256-bit, a notable boost over the 64- little and also 128-bit secrets utilized in the WEP system.
A number of the notable changes executed with WPA featured information integrity examinations (to identify if an assaulter had actually captured or even changed packages passed in between the gain access to the point as well as a customer) as well as the Temporal Trick Honesty Procedure (TKIP). TKIP employs a per-packet key system that was significantly much more protected than dealt with secret used in the WEP body. TKIP was eventually replaced through Advanced Security Criterion (AES).
Regardless of what a considerable renovation WPA was over WEP, the ghost of WEP spooked WPA. TKIP, a central component of WPA, was made to be quickly presented using firmware upgrades onto existing WEP-enabled devices. Hence it had to reuse particular components utilized in the WEP unit which, ultimately, were also capitalized on.
WPA, like its ancestor WEP, has been shown through both proof-of-concept and applied public exhibitions to become vulnerable to invasion. Fascinatingly the procedure where WPA is generally breached is certainly not a direct attack on the WPA protocol (although such attacks have been efficiently shown) yet by attacks on an auxiliary unit that was presented along with WPA, Wi-Fi Protected Arrangement (WPS), made to make it simple to connect devices to contemporary gain access to points.

WPA2

WPA has, since 2006, been formally displaced by WPA2. Among the absolute most significant improvements in between WPA and WPA2 was the necessary use of AES formulas and also the intro of CCMP (Counter Cipher Method with Block Chaining Information Verification Code Process) as a replacement for TKIP (still kept in WPA2 as a fallback unit as well as for interoperability along with WPA).
Currently, the critical security vulnerability to the real WPA2 device is an obscure one (and also requires the attacker to now have accessibility to the gotten Wi-Fi network to access to specific tricks and then bolster an attack against various other gadgets on the system). Therefore, the security implications of the well-known WPA2 vulnerabilities are restricted just about entirely to venture level networks and be entitled to little to no efficient consideration about residence network security.
Regrettably, the very same susceptibility that is the most significant opening in the WPA shield, the attack vector using the Wi-Fi Protected Setup (WPS), continues to be in modern WPA2- qualified access points. Although getting into a WPA/WPA2 secured network utilizing this weakness requires anywhere from 2-14 hrs of sustained effort with a modern-day computer, it is still a genuine security problem. WPS should be impaired (as well as, possibly, the firmware of the get access to factor need to be flashed to a distribution that doesn't even promote WPS, so the attack angle is cleared away).

The following is a simple list placing the current Wi-Fi security procedures, ordered coming from ideal to worst:

1. WPA2 +AES
2. WPA +AES
3. WPA + TKIP/AES (TKIP is there as a fallbackmethod)
4. WPA +TKIP
5. WEP
6. Open Network (no security atall)

IV. CONCLUSION

Preferably, Wi-Fi Protected Configuration (WPS) are going to be handicapped as well as the level of security readied to WPA2 +AES. Every little thing else on the checklist is a less than ideal walk out from that. Depending On to ABI Research, a technology investigation and advising firm, greater than 30 billion tools will be wirelessly linked to the Web of Traits (Web of Whatever) through 2020.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 11, November 2020 ||

REFERENCES

1. MinistryofInternalAffairsandCommunications:2015 WhitePaperon Information and Communications in Japan—Past,Present,andFutureofICT.July28,2015 (in Japanese). http://www.soumu.go.jp/johotsusintokei/whitepaper/ h27.html
2. Fujitsu:FujitsuTechnologyandServiceVision.http://www.fujitsu.com/global/vision/
3. ARIB2020andBeyondAdHocGroup:WhitePaper— MobileCommunicationsSystemsfor2020andbeyond. Ver. 1.0.0. October 8, 2014.
4. TTC:"AdHoc Groupon Future Mobile Networking" White Paper. Ver. 1.0 March 2015. http://www.ttc.or.jp/files/5514/2856/3199/ White_paper_on_Future_Mobile_Networking_by_ TTC_20150409.pdf
5. Sugandhi Maheshwaram, "A Review on Deep Convolutional Neural Network and its Applications", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 8, Issue 2, February 2019
6. Sugandhi Maheshwaram, "A Comprehensive Study on the Advantages and Features of MVC Architecture", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 8, Issue 1, January 2020
7. Sugandhi Maheshwaram, "CLOUD DEPLOYMENT STRATEGIES AND CONCEPTUAL VIEW OF CLOUD COMPUTING", Alochana Chakra Journal, Volume VIII, Issue VI, June2019
8. Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions", International Journal of Information Technology and Management Vol. XI, Issue No. XVII, November-2016,
9. Sugandhi Maheshwaram, "A STUDY ON THE CHALLENGES IN HANDLING BIG DATA", International Journal of Research, Volume VIII, Issue III, March 2019
10. Sugandhi Maheshwaram, "A STUDY ON THE CONCEPT AND EVOLUTION OF MACHINE LEARNING", INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY, Volume-11,Issue-5, May-19
11. Sugandhi Maheshwaram, "A Novel Technique for Preventing the SQL Injection Vulnerabilities", International Journal of Research and Applications, Volume 5, Issue 19, July-Sep 2018
12. Sugandhi Maheshwaram, "A Study on Security Information and Event Management (SIEM)", International Journal of Research and Applications, Volume 5, Issue 17, Jan-Mar 2018
13. Sugandhi Maheshwaram, "A Study Design of Big Data by Concentrating on the Atmospheric Information Evaluation", International Journal for Scientific Research & Development, Vol. 7, Issue 03, 2019
14. Sugandhi Maheshwaram, "Architectural Framework of Cloud Computing Environment", International Journal of Scientific Research in Science, Engineering and Technology, Volume 4, Issue 1, January-February2018
15. Sugandhi Maheshwaram, "An Overview of Open Research Issues in Big Data Analytics", Journal of Advances in Science and Technology, Vol. 14, Issue No. 2, September-2017
16. Sugandhi Maheshwaram, "CLOUD DEPLOYMENT STRATEGIES AND CONCEPTUAL VIEW OF CLOUD COMPUTING", Alochana Chakra Journal, Volume VIII, Issue VI, June2019
17. Sugandhi Maheshwaram, "A Study on Vulnerabilities, Applications, Advantages and Routing Protocols in MANET", International Journal of Scientific Research in Science and Technology, Volume 4, Issue 1, January-February2018
18. Sugandhi Maheshwaram, "An Overview towards the Techniques of Data Mining", RESEARCH REVIEW International Journal of Multidisciplinary, Volume04, Issue02, February 2019
19. Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.
20. Sudheer Kumar Shriramoju, "Review on NoSQL Databases and Key Advantages of Sharepoint", International Journal of Innovative Research in Science, Engineering and Technology, ISSN(Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, November 2018.
21. Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint On Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2, Issue 6, November-December-2017.
22. Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016
23. Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014
24. Sudheer Kumar Shriramoju, "A Comprehensive Review on Database Security Threats and Visualization Tool for Safety Analyst", International Journal of Physical Education and Sports Sciences, Vol. 14, Issue No. 3, June-2019
25. Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

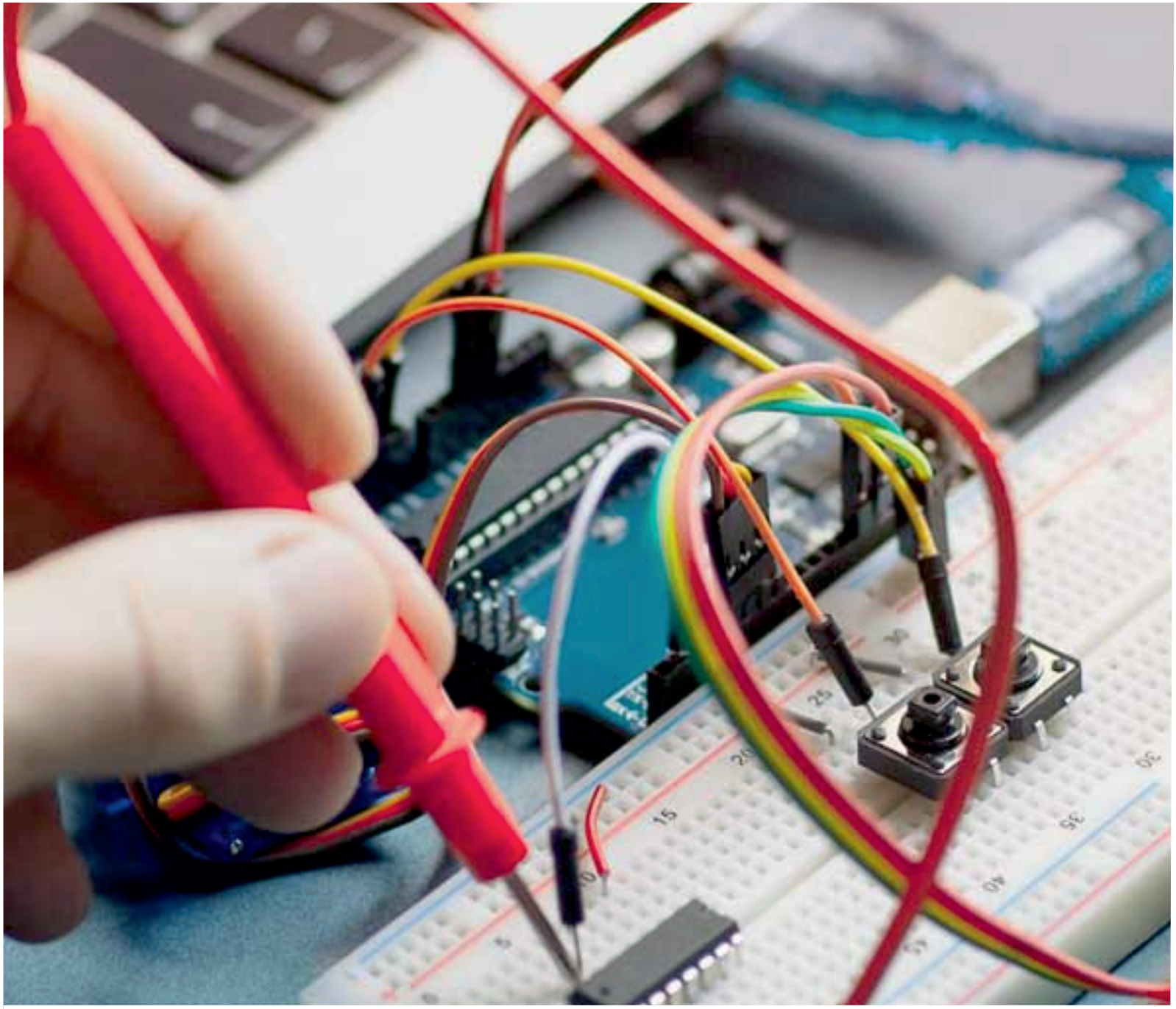
|| Volume 9, Issue 11, November 2020 ||

Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012
26. Sudheer Kumar Shriramoju,, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013
27. Sudheer Kumar Shriramoju, "Security Challenges of Service and Deployment Models", International Journal of Scientific Research in Science and Technology, Volume 4, Issue 8, May-June2018
28. Sudheer Kumar Shriramoju, "A REVIEW ON DIFFERENT TYPES OF VIRTUALIZATION AND HYPERVISOR", Alochana Chakra Journal, Volume VIII, Issue II, February 2019
29. Sudheer Kumar Shriramoju, "Cloud security - A current scenario and characteristics of cloud computing", International Journal of Research and Applications, Volume 5, Issue 18, Apr-Jun 2018
30. Sudheer Kumar Shriramoju, "SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING", Airo International Research Journal, Volume IX, Feb 2017.
31. Malyadri. K, "Architecture and Components of Cloud-Based ML Framework", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 8, Issue 1, January 2019
32. Malyadri. K, "An Overview towards the Different Types of Security Attacks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2014
33. Malyadri. K, "Security Threats, Security Vulnerabilities and Advance Network Security Policies", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 9, September 2013
34. Malyadri. K, "Need for Key Management in Cloud and Comparison of Various Encryption Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology , volume 1, issue 1, July-August 2016
35. Malyadri. K, "Cloud-Based Ml Framework Working with Analytic Tools", International Journal of Scientific Research in Science and Technology, Volume 6, Issue 6, November-December-2019
36. Malyadri. K, "Integration of Appropriate Analytic tools towards Mobile Technology Development", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 6, Issue 6, June 2018
37. Malyadri. K,"A STUDY ON EXPERIENCES ANDLIMITATIONS OF MOBILE COMMUNICATION", Alochana Chakra Journal, Volume VI, Issue VIII, August2017
38. Malyadri.K, PUSHPAVATHI MANNAVA, "A COMPREHENSIVE REVIEW ON MOBILE E-SERVICETECHNOLOGY", Alochana Chakra Journal, Volume IX, Issue II, February 2020
39. Malyadri. K,"CHALLENGES CONCERNING MOBILEDEVELOPMENT AND MODEL-DRIVEN DEVELOPMENT OF MOBILE APPS", Airo International Research Journal, volume XVI, Nov 2018
40. Malyadri, N. Surya Teja, "Related technologies and the role of mobile app development life cycle", International Journal of Research and Applications, Volume 5, Issue 17, Jan-Mar 2018.
41. Malyadri K, Surya Teja N, "Key characteristics of mobile applications and trends in mobile app Industry", International Journal of Research and Applications, Volume 7, Issue 25, Jan-Mar 2020.
42. Bhagya Rekha Kalukurthi, "A Comprehensive Review on Challenges and Types of Big Data", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 7, Issue 1, January 2018.
43. Rakesh Rojanala, "Generic Working of an Artificial Neuron and Its Output Mathematical Representation", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 8, Issue 1, January 2019.
44. Yeshwanth Valaboju, "A Study on Cryptosystem Types and Cryptographic Principles", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 6, June 2016
45. Rakesh Rojanala, "Components of Data Mining and Big Data Analytics in Intra-Data Center Networks", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 7, July 2016
46. Rakesh Rojanala, "An Overview of Intrusion Detection System and the Role of Data Mining in Information", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 6, Issue 3, March 2017
47. Bhagya Rekha Kalukurthi, "A Comprehensive Review on Machine Learning and Deep Learning", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 8, Issue 6, June 2019
48. Bhagya Rekha Kalukurthi, "Regulatory Compliance and Supervision towards Artificial Intelligence", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 12, December 2019
49. Yeshwanth Valaboju, "Capabilities and Key Benefits of Sap NetWeaver Gateway", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 1, January 2019
50. Rakesh Rojanala, "Machine Learning: Intersection of Statistics and Computer Science", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 8, August 2017
51. Malyadri. K, "A Review on Radio Transmission Technology and Principles of Wireless Networking", International Journal of Scientific Research in Science and Technology, Volume 1, Issue 3, July-August 2015

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 11, November 2020 ||

52. BhagyaRekha Kalukurthi, "Data Mining Strategy for Discovering Intriguing Patterns and Challenges with Bigdata for Global Pulse Development", International Journal of Scientific Research in Science and Technology, Volume 3, Issue 3, March-April-2017
53. Yeshwanth Valaboju, "A Review on The Database Security Requirements and Guidelines", International Journal of Scientific Research in Science and Technology, Volume 3, Issue 6, July-August2017
54. Rakesh Rojanala, "Cloud Computing Characteristics and Deployment of Big Data Analytics in The Cloud", International Journal of Scientific Research in Science and Technology, Volume VIII, Issue II, March-April2014
55. Rakesh Rojanala, "Cloud-Based ML Framework Built Using Apache Ecosystem", International Journal of Scientific Research in Science, Engineering and Technology, Volume 7, Issue 1, January-February2020
56. BhagyaRekha Kalukurthi, "Big Data Classification and Methods of Data Mining, Big Data", International Journal of Scientific Research in Science, Engineering and Technology, Volume 3, Issue 5, July-August2017
57. Rakesh Rojanala, "Algorithms, Models and Applications on Artificial Intelligence", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 5, Issue 4, July-August 2019
58. Yeshwanth Valaboju, "IOT Communication Technologies and Future of Internet of Things", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 6, November-December 2017
59. BhagyaRekha Kalukurthi, "A Study on The Big Data Characteristics", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 1, Issue 1, July-August 2016
60. Bhagya Rekha Kalukurthi, "Security Vulnerabilities, Security Threats, and Advance Network Security Policies", Journal of Interdisciplinary Cycle Research, Volume VI, Issue I, Jan-June2014
61. Bhagya Rekha Kalukurthi, "IMPLEMENTATION OF BIG DATA ANALYTICS AND BIG DATAGOVERNANCE", The International journal of analytical and experimental modal analysis, Volume VII, Issue I, May2015
62. Rakesh Rojanala, "CLOUD COMPUTING ARCHITECTURAL FRAMEWORK", Journal of Interdisciplinary Cycle Research, Volume V, Issue I, Jan-June2013
63. Rakesh Rojanala, "AN OVERVIEW ON CLOUD COMPUTING MODELS AND CLOUD DELIVERY MODELS", The International journal of analytical and experimental modal analysis, VolumeIV, Issue I,JAN-JUNE2012
64. Rakesh Rojanala, "A COMPREHENSIVE STUDY ON THECHALLENGES OF STREAM DATA MINING AND BIG DATA-ORIENTED STREAM DATAMINING", The International journal of analytical and experimental modal analysis, Volume VII, Issue II, July-December2015
65. Yeshwanth Valaboju, "A LITERATURE REVIEW ON NEURAL NETWORKARCHITECTURES", Journal of Interdisciplinary Cycle Research, Volume VII, Issue II, December2015
66. Yeshwanth Valaboju, "AN OVERVIEW ON THE TYPES OF PASSWORD AND DOS ATTACKS", Journal of Interdisciplinary Cycle Research, Volume IX, Issue XI, November2018
67. Yeshwanth Valaboju, "AN OVERVIEW ON SAP FIORI DESIGN PRINCIPLES AND FIORI ARCHITECTURE FOR ANALYTICAL APPLICATIONS", The International journal of analytical and experimental modal analysis, Volume X, Issue IX, September2018



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.122

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details